

**THE UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF MISSOURI**

**IN THE MATTER OF THE  
SEARCH OF:  
A RED APPLE IPHONE  
SEIZED ON JULY 19, 2019, FROM  
DANIEL RANDOLPH STONE-TAYLOR**

Case No.

19-SW-2112 DPR

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Brian Martin, a Task Force Officer (TFO) with the Homeland Security Investigations, Immigration and Customs Office (HSI/ICE), being first duly sworn, hereby depose and state as follows:

1. I have been employed as a deputy sheriff with the Barry County, Missouri, Sheriff's Office, since 1997 and a sworn law enforcement officer since 1985. I am assigned as a TFO with HSI/ICE and a member of the Southwest Missouri Cyber Crimes Task Force (SMCCTF) headquartered in Joplin, Missouri. As an investigator with these entities, I have been tasked to investigate computer crimes, including violations against children. I have gained expertise in the conduct of such investigations through training in seminars, classes, and everyday work related to conducting these types of investigations. I have attended trainings provided by the Internet Crimes Against Children Program, the Federal Bureau of Investigation's Regional Computer Forensic Laboratory, and the Missouri Internet Crimes Against Children (ICAC) Task Force. I have authored, executed, or assisted in over 200 search warrants on the state and federal level.
2. As part of this affiant's duties with HSI/ICE, this affiant investigates criminal violations relating to child exploitation, child pornography, and coercion and enticement, in violation of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422.
3. The statements in this affidavit are based on my personal observations, training and

experience, investigation of this matter, and information obtained from other agents and witnesses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, this affiant has not included each and every fact known to me concerning this investigation. This affiant has set forth the facts necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422 are currently located within a red Apple iPhone, seized on July 19, 2019, from Daniel Randolph Stone-Taylor, currently stored at the SMCCTF Cyber Crimes Lab located at 303 East 3<sup>rd</sup> Street, Joplin, Missouri 64801, a location within the Western District of Missouri.

4. This affidavit is in support of an application for a search warrant for evidence, fruits, and instrumentalities of the foregoing criminal violations, which relate to the knowing possession, receipt, distribution, and/or production of child pornography, and coercion and enticement of a minor. The property to be searched is described in the following paragraphs and fully in Attachment A. This affiant requests the authority to search and/or examine the seized items, specified in Attachment B, as instrumentalities, fruits, and evidence of crime.

5. This affiant has probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422, involving the use of a computer, in or affecting interstate commerce, to receive, distribute, possess, and/or produce child pornography, and coercion and enticement of a minor, are located in and within the aforementioned property described below. Thus, as outlined below, and based on my training and experience, there is probable cause to believe that evidence, fruits, and/or instrumentalities of the aforementioned crimes are located in this property.

#### **STATUTORY AUTHORITY**

6. This investigation concerns alleged violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422 relating to material involving the sexual exploitation of minors:

- a. 18 U.S.C. § 2251(a) prohibits a person from employing, using, persuading, inducing, enticing, or coercing a minor to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce, or if such visual depiction actually was transported in or affecting interstate commerce.
- b. 18 U.S.C. § 2252 prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.
- c. 18 U.S.C. § 2252A prohibits a person from knowingly mailing, transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.
- d. 18 U.S.C. § 2422 prohibits an individual using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States from knowingly persuading, inducing, enticing, or coercing any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so.

### DEFINITIONS

7. The following definitions apply to this Affidavit and its Attachments:
- a. The term “minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.
  - b. The term “sexually explicit conduct,” 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.
  - c. The term “visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.
  - d. The term “computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
  - e. The term “child pornography,” as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:



1. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
2. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
3. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

f. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, and painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies), mechanical form (including, but not limited to, phonograph records, printing, and typing) or electrical, electronic, or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

g. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications

equipment.

h. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.

i. “Domain names” are common, easy to remember names associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

j. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transfer Protocol (HTTP).

#### **CELLULAR PHONES AND CHILD PORNOGRAPHY**

8. Based on this affiant’s knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom this affiant has had discussions, cellular phones have likewise revolutionized the manner in which child pornography is produced and distributed.

9. Cellular phones (“cell phones”) are exceptionally widespread. The Central Intelligence Agency estimates that in 2016 there were 416 million cell phone subscribers in the United States.

Cell phones increasingly offer features such as integrated digital cameras, the ability to store hundreds of digital images, and the ability to access and browse the Internet.

10. In this affiant's training and experience, the ready availability and personal nature of cell phones has led to their frequent use in the commission of child pornography offenses. Individuals with a sexual interest in children will often use their cell phone to browse the Internet and to distribute, receive, and store child pornography files. Individuals producing child pornography will also frequently use the integrated digital camera within a cell phone to produce the images, and then store the images both on the phone and on other devices – such as computers and computer storage media.

11. Cell phones, like other computer systems, will frequently retain data relating to activities, such as Internet browsing history, digital images, and other digital data, that can remain stored for a long period of time.

#### **SPECIFICS OF SEARCH AND SEIZURE OF CELL PHONES**

12. Searches and seizures of evidence from cell phones commonly require agents to download or copy information from the devices and their components, or seize most or all items to be processed later by a qualified computer expert in a laboratory or other controlled environment.

This is almost always true because of the following two reasons:

a. Computer storage devices, including cellular phones, can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to

accomplish fully on-site.

b. Searching cell phones for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computing system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since digital/electronic evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

13. Furthermore, because there is probable cause to believe that the cell phone is an instrumentality of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, as well as 18 U.S.C. § 2422, and it should be seized as such.

#### **BACKGROUND OF INVESTIGATION**

14. On July 19, 2019, Bolivar, Missouri, Police Department Corporal Dawnielle Robinson reported that a 20-year-old male, Daniel Stone-Taylor, had driven to a location near Bolivar, Polk County, Missouri, from his residence in Conway, Arkansas, for the purpose of picking up a 12-year-old female (hereinafter referred to as “Jane Doe”).

15. Cpl. Robinson reported that after the Conway, Arkansas, Police Department (CPD) had been notified that Jane Doe was believed to be with Stone-Taylor, Stone-Taylor was stopped a short time later in a red Hyundai Elantra near his residence in Conway. Law enforcement located Jane Doe in the vehicle with Stone-Taylor.



16. Post-*Miranda*, Stone-Taylor told CPD Officer Chuck Myers that he had driven to Missouri on July 17, 2019, to pick up Jane Doe, and he returned with her to his home in Conway. Stone-Taylor said he believed Jane Doe was 16 years old when he initially met her; however, he admitted that this was not the first time he had gone to Missouri to pick Jane Doe up and bring her to Arkansas. Stone-Taylor said that during Jane Doe's spring break from school in March 2019, he brought her to his apartment in Conway for four days, and then returned her home to Missouri. Stone-Taylor said that he and Jane Doe had engaged in sexual activity including digital and penile penetration of Jane Doe's vagina and oral sex on both occasions Jane Doe was in Conway. Stone-Taylor explained that he and Jane Doe had also exchanged pornographic images, some of which he asked for using the SnapChat application.
17. Officer Myers seized two cellular phones. A red Apple iPhone was seized from Stone-Taylor's person and a white Apple iPhone was seized from Jane Doe. Officer Myers entered both cell phones into evidence.
18. During a follow-up post-*Miranda* interview with CPD Detective Taylor Sullivan, Stone-Taylor said that he had saved several of the pictures that Jane Doe had sent to him via SnapChat on his cell phone.
19. During an initial interview with law enforcement, Jane Doe said that she and Stone-Taylor had been communicating online for some time. Jane Doe stated that she had arranged to meet Stone-Taylor so she could leave with him and travel to Arkansas. Jane Doe admitted to engaging in sexual activity with Stone-Taylor, including sexual intercourse and oral sex. Jane Doe said this was the second time she had been to Stone-Taylor's apartment.
20. During a forensic interview on July 19, 2019, at the Child Advocacy Center in Springfield, Missouri, Jane Doe disclosed that she had traveled to Arkansas with Stone-Taylor earlier that week

and that they engaged in sexual activity while in his apartment. Jane Doe also described that she had spent four days with Stone-Taylor at his apartment in Conway during her school's spring break. This affiant confirmed with Jane Doe's school that spring break was between March 15, 2019, and March 24, 2019.

21. On July 29, 2019, this affiant made contact with CPD Detective Sullivan in Harrison, Arkansas. Detective Sullivan transferred custody of Stone-Taylor's red Apple iPhone and Jane Doe's white Apple iPhone to this affiant. This affiant transported the cellular phones to the SMCCTF Cyber Crime Lab, 303 East 3<sup>rd</sup> Street, Joplin, Missouri 64801, where the phones are currently being stored. Stone-Taylor's cellular phone is red in color with no visible serial number on the outside cover. The words "iPhone" and "(Product)," in silver color marking, are located on the back of the phone.

**PROBABLE CAUSE**

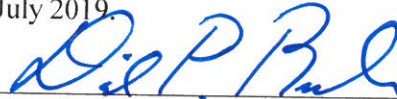
22. Based on the above facts, this affiant believes probable cause exists for the issuance of a warrant to search the premises described more fully in Attachment A for (1) property that constitutes evidence of the commission of a criminal offense; (2) contraband, the fruits of a crime, or things otherwise criminally possessed; and/or (3) property designated or intended for use or which is or has been used as the means of committing a criminal offense, namely possible violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422 including, but not limited to, the items listed in Attachment B.

Further Affiant Sayeth Naught.



Brian Martin  
Task Force Officer  
Homeland Security Investigations

Sworn to and subscribed to me this 31<sup>st</sup> day of July 2019.



DAVID P. RUSH  
United States Magistrate Judge  
Western District of Missouri